

Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»

# МАТЕМАТИКА В СУЧАСНОМУ ТЕХНІЧНОМУ УНІВЕРСИТЕТІ

Матеріали  
VIII Міжнародної  
науково-практичної конференції  
*Київ, 26–27 грудня 2019 року*

Вінниця  
2020

**УДК 51(082)**  
**М34**

**Матеріали** VIII Міжнар. наук.-практ. конф. «Математика в сучасному технічному університеті», Київ, 27–28 грудня 2019 р. — Вінниця: Видавець ФОП Кушнір Ю. В., 2020. — 336 с. — Укр., рос., англ., білорус.

**Материалы** VIII Межд. науч.-практ. конф. «Математика в современном техническом университете», Киев, 27–28 декабря 2019 г. — Винница: Видавець ФОП Кушнір Ю. В., 2020. — 336 с. — Укр., рус., англ., белорус.

**Proceedings** of Eighth International Scientific-Practical Conference “Mathematics in Modern Technical University”, Kyiv, December, 27–28, 2019. Vinnytsia: Publisher FOP Kushnir Yu. V., 2020. 336 pp.

**ISBN 978-617-7721-27-6**

**Програмний комітет**

VIII Міжнародної науково-практичної конференції «Математика в сучасному технічному університеті»:

Проф. О. І. Клесов (Київ, Україна), (голова)  
Проф. Н. О. Вірченко (Київ, Україна)  
Проф. О. В. Іванов (Київ, Україна)  
Проф. П. В. Задерей (Київ, Україна)  
Доц. О. О. Диховичний (Київ, Україна)

**Організаційний комітет**

Міжнародної науково-практичної конференції «Математика в сучасному технічному університеті»

Доц. В. О. Гайдей (Україна), голова  
В. В. Бовсуновська (Київ, Україна)  
Ю. Є. Приходько (Київ, Україна)

УДК 51(082)

*Матеріали подано в авторській редакції*

**ISBN 978-617-7721-27-6**

©Автори

©КПІ ім. Ігоря Сікорського, 2020



# ЗАСТОСУВАННЯ МАТЕМАТИКИ В СУМІЖНИХ НАУКАХ

## **Застосування фракталів в інформаційній та кібернетичній безпеці**

**Ю. Д. Жданова, С. О. Спасітелєва, С. М. Шевченко**

*Київський університет імені Бориса Грінченка, Київ, Україна*

*y.zhdanova@kubg.edu.ua, s.spasitielieva@kubg.edu.ua,*

*s.shevchenko@kubg.edu.ua*

У доповіді розглянуті підходи до застосування фрактального аналізу в інформаційній та кібернетичній безпеці, які можуть бути використані при підготовці фахівців у процесі науково-дослідної роботи.

**Ключові слова:** фрактал, властивості фракталів, моделі фракталів, інформаційна та кібернетична безпека, захист інформації.

Сучасний захист інформації виходить за рамки детермінованої системи з визначеними характеристиками. Відбувається це у зв'язку з тим, що система обробки інформації належить до самоорганізуючих систем, і, з точки зору синергетики, найменші відхилення середніх показників приводить не тільки до нових властивостей системи сучасні, але й до появи нової системи в цілому, до так званого «детермінованого хаосу». Для дослідження таких систем активно застосовують сучасні методи і підходи, зокрема ті, що пов'язані з математичною теорією фракталів.

Одною з характерних ознак фрактальних структур є самоподібність, що може проявлятися не тільки через фізичні форми, а й через фрактальну поведінку. Фрактали дозволяють моделювати складні природні форми та процеси за допомогою простих ітераційних процедур. Тому теорія фракталів на сьогодні є актуальною та затребуваною у різних галузях наукових досліджень.

Спектр застосування теорії фракталів є надзвичайно широким. Її активно використовують у комп'ютерній графіці для зображення об'єктів природи. Базою для побудови таких фракталів є математична формула в пам'яті комп'ютера. У фізиці цей інструментарій використовують для моделювання нелінійних процесів: хмари, турбулентність, вогонь тощо; у біології — для моделювання популяцій.

В останні часи фрактальну геометрію широко використовують в економіці та фінансах, наприклад, для аналізу біржових ринків.

У часи цифрового суспільства, у сфері інформаційної безпеки фрактальну геометрію застосовують для генерації складних об'єктів на дисплеях, стисканні даних, опису соціальних процесів тощо.

Застосування фракталів у задачах забезпечення захисту інформації розглянуто у працях Локтев та Залетдинов (2010), Никонов та Зобов (2017).

Є очевидним, що розвиток суспільства з кожним днем стає залежним від розвитку інформаційно-комунікаційних технологій, від зростаючої ролі інформації в життєвому просторі людства. Тому саме захист цієї інформації є першочерговим завданням у сучасному світі. Для вирішення поставленого завдання необхідно постійно розвивати професійні компетенції фахівців інформаційної та

кібернетичної безпеки, що неможливе без удосконалення змісту їх освіти, перенесення сучасного математичного апарату, зокрема фрактального аналізу, у підготовку майбутніх спеціалістів.

На сучасному етапі у зв'язку з недостатньою надійністю програмних реалізацій криптографічних алгоритмів, наукові кола світу ведуть розробки по створенню та впровадженню альтернативних методологій захисту інформації, зокрема таких, які ґрунтуються на використанні перспективних напрямів математики, — фрактального моделювання.

Розгляньмо різні підходи застосування теорії фракталів в інформаційній та кібернетичній безпеці, які можуть бути впровадженні в навчальний процес підготовки майбутніх фахівців у даній галузі.

У дослідженні (Локтев & Залетдинов, 2010) пропонується розглядати безпеку кожного автоматизованого робочого місця мережі за допомогою набору властивостей, які можуть бути представлені у вигляді фракталів. Потім, використовуючи їх самоподібність, спроектувати одержані результати на всю систему захисту інформації. Учені пропонують використовувати фрактали на трьох етапах:

- 1) перший фрактал розкриває можливості нанесення шкоди інформації;
- 2) другий фрактал описує вимоги по захисту інформації;
- 3) третій фрактал представляє можливості захисту інформації у комп'ютерній мережі.

Надалі вводиться топологічне дерево, яке описує зв'язок між окремими автоматизованими робочими місцями персоналу. Кожне місце містить чотири частини: технічне забезпечення, програмне забезпечення, інформаційне забезпечення, організаційно-методичне забезпечення. Таким чином, визначивши параметри одного автоматизованого робочого місця, можна змодельовати систему захисту інформації у вигляді набору фракталів для корпоративної мережі. Даний підхід описує симетричні системи захисту інформації, де до кожного елементу системи висуваються однакові вимоги.

Аналіз наукової роботи Никонов та Зобов (2017) дозволив виділити приклади можливого застосування фрактальних відображень для породження довгих неперіодичних послідовностей, які використовують в теорії шифрування. Як відомо, фрактальні об'єкти, одержані за допомогою нелінійних динамічних функцій, за своєю складністю наближаються до об'єктів природних. Це дозволяє використовувати ці функції як надійних датчиків псевдовипадкових послідовностей будь-якої довжини. Фрактальні функції, маючи вхідні аргументи у вигляді набору символів, можуть відобразити їх на числову послідовність. Здійснити аналіз цієї послідовності практично неможливо. Проте, знаючи вихідну функцію та її початкові параметри, можливо легко відновити початковий набір символів. Розв'язання оберненої задачі не є можливим. У статті представлені різні методи побудови фракталів як уже відомих, так і нових фрактальних конструкцій, зокрема з використанням порогових операцій.

Взагалі, слід відмітити, що теорія фракталів саме найчастіше застосовується

в алгоритмах шифрування. Наприклад, для реалізації шифрів заміни та підстановки; як фактор, що вносить додаткову невизначеність при використанні генератора псевдовипадкових чисел або використаний замість генератора псевдовипадкових чисел; для зниження ймовірності одержання ключа та інші. Найчастіше використовують добре досліджені й вивчені множини Мандельброта та Жюліа (Зайцева & Скобелев, 2007).

Наукове дослідження Назаркевич та ін. (2015) присвячене розробці методу захисту документів латентними елементами на основі фракталів. Ученими представлено спеціальні графічні побудови, на основі яких створено латентні елементи, що підвищують ефективність та надійність захисту. Спосіб захисту полягає в тому, що у векторному форматі утворюють графічні елементи захисної сітки, які копіюють, розмножують та утворюють захисну сітку на основі фракталу за допомогою рекурсивної процедури. Фрактали будуються рекурсивною процедурою, де кожен одиничний графічний елемент постає в ролі генератора, який задає величину захисного елемента. Величина захисного елемента будується мінімально можливою для відтворення в друкованому виді, а потім ініціатором заповнюється площа сітки. Побудова сітки починається із задання параметрів фракталу. На основі створеного фракталу можна створити велику кількість варіантів фрактальних сіток, змінюючи масштаб, поворот, а також збільшуючи або зменшуючи кількість ітерацій. Фрактальні фонові сітки є складними для відтворення, адже при цьому необхідно використати алгоритм побудови вибраного типу фракталу, шаблон якого відомий тільки розробнику.

Детальніше з аналізом існуючих підходів до використання фрактального аналізу в області захисту інформації можна ознайомитися у статті Шевченко та ін. (2019).

Останнім часом для підвищення рівня безпеки IoT, зокрема пристроїв розумного будинку, визначають застосування технології Блокчейн (Dorri et al., 2017; Fan et al., 2018)

Блокчейн інтегрує такі технології, як розподілене зберігання даних, однорангова передача, механізм консенсусу та алгоритм шифрування. Очікується, що це дозволить не тільки усунути слабкість безпеки IoT, але й знизити експлуатаційні та кредитні витрати централізованої мережі, підвищити операційну ефективність та використання промислових активів. Науковою школою студентів та викладачів кафедри Інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка ведуться розробки системи безпеки пристроїв розумного будинку на основі технології Блокчейн із застосуванням фрактального аналізу.

Потужні математичні розробки, добра алгоритмізація функцій дозволяє ефективно використовувати теорію фракталів для захисту інформації. На сьогодні існує достатня кількість уже реалізованих алгоритмів фрактального моделювання у вигляді програмного забезпечення. Проте, використання різних моделей фракталів для створення надійних систем захисту інформації потребує подальшого вивчення.

Розглянуті підходи до застосування фрактального аналізу в інформаційній та кібернетичній безпеці можуть бути використані при підготовці фахівців у процесі науково-дослідної роботи або при написанні курсової чи дипломної роботи.

### Список літератури

- Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618–623). IEEE. <https://allquantor.at/blockchainbib/pdf/dorri2017blockchain.pdf>
- Fan, S., Song, L., & Sang, C. (2019, October). Research on Privacy Protection in IoT System Based on Blockchain. In *International Conference on Smart Blockchain* (pp. 1–10). Cham: Springer. [https://easychair.org/publications/preprint\\_download/Vg7v](https://easychair.org/publications/preprint_download/Vg7v)
- Зайцева, Э. Е. & Скобелев, В. Г. (2007). Шифр на основе отображения Мандельброта. *Вестник Томского университета. Приложение*, (23). 107–113.
- Локтев, А. А., & Залетдинов, А. В. (2010) Использование фракталов в задачах обеспечения информационной безопасности. *Вестник Тамбовского университета. Серия: Естественные и технические науки*, 15(2), 599–604. <http://journals.tsutmb.ru/go/1810-0198/2010/2/599-604/>
- Назаркевич, М. А., Дронюк, І. М., Троян, О. А. & Томащук, Т. Ю. (2015). Розробка методу захисту документів латентними елементами на основі фракталів. *Захист інформації*, 17(1), 21–26. <https://doi.org/10.18372/2410-7840.17.7505>
- Никонов, В. Г., & Зобов, А. И. (2017). О возможности применения фрактальных моделей при построении систем защиты информации. *Computational nanotechnology*, (1), 39–49.
- Шевченко, С. М., Жданова, Ю. Д., Спасітєлева, С. О., Негоденко, О. В., Мазур, Н. П. & Кравчук, К. В. (2019). Математичні методи кібербезпеки: фрактали та їх застосування в інформаційній та кібербезпеці. *Кібербезпека: наука, освіта, техніка*, 1(5), 31–39. <https://doi.org/10.28925/2663-4023.2019.5.3139>

# ЗМІСТ

## Секція 1. Застосування математики в суміжних науках

Borysenko O. V. <i>Stochastic mutualism model of population dynamics</i> .....	4
Golinko I., Galytska I. <i>Passive identification of the plant time response for an acting control system</i> .....	8
Goy T. <i>Jacobsthal number identities using the generalized Brioschi formula</i> .....	13
Kovalchuk V. V. <i>Lagrange's equation for a triple inverted pendulum</i> .....	18
Антоненко Н. М., Ткаченко І. Г., Морозов Ю. В. <i>Про один підхід до розв'язання осесиметричної задачі теплопровідності для багатошарової основи з неідеальним тепловим контактом між шарами</i> .....	22
Баліна О. І., Безклубенко І. С., Буценко Ю. П. <i>Управління потокорозподілом інженерної мережі в аварійній ситуації</i> .....	25
Бовсуновська В. В., Задерей П. В., Задерей Н. М., Нефьодова Г. Д. <i>Про нерівність Лебега — Ландау на класах <math>\psi</math>-диференційовних функцій</i> .....	28
Буценко Ю. П., Лабжинський В. А. <i>Кластерний підхід до діагностування складних систем</i> .....	32
Буценко Ю. П., Савченко Ю. Г. <i>Марківська модель технічного стану в електронних пристроях із структурною надлишковістю</i> .....	34
Голуб В. П. <i>Определение параметров ядер наследственности в линейной теории вязкоупругости методом интегрального преобразования Лапласа — Карсона</i> .....	38
Горалік Є. Т., Крюков М. М., Лупіна Т. О. <i>Рух рятувальної шлюпки вільного падіння при сходженні з похилої рампі</i> .....	43
Горленко С. В. <i>До обернення теореми Гріна</i> .....	48
Демидюк М. В., Демидюк В. М. <i>Використання методу Понтрягіна в задачі оптимального керування дволанковим маніпулятором</i> .....	51
Диховичний О. О., Круглова Н. В. <i>Система для аналізу й побудови психологічних опитувальників та визначення точних цільових психологічних профілів</i> .....	56
Довгай В. В. <i>Оцінка розв'язків неавтономної системи лінійних диференціальних рівнянь другого порядку</i> .....	59
Донецький С. В. <i>Співіснування атракторів у системі генератор-п'єзокерамічний випромінювач</i> .....	63
Жданова Ю. Д., Спасітелєва С. О., Шевченко С. М. <i>Застосування фракталів в інформаційній та кібернетичній безпеці</i> .....	67
Задерей П. В., Задерей Н. М., Нефьодова Г. Д., Хрипко С. С. <i>Про ряди Фур'є обмежених функцій</i> .....	71
Зеленський А. Г., Побігай Є. Д., Томін А. Ю., Фомін О. С. <i>Застосування математики в розрахунках однорідних і тришарових прямокутних пластин на згин</i> .....	73
Игнатьев А. О. <i>Динамика взаимодействия вирусов и иммунной системы</i> .....	76



Іваненко Т. В. Математичне моделювання інвестиційного проєкту як функції $n$ змінних .....	80
Іваненко Т. В., Тимошенко О. А. Детермінована задача прийняття оптимального рішення при виборі інвестиційного проєкту.....	85
Кобзар Ю. М. Моделювання процесу руйнування внаслідок втоми за умов багато циклового навантаження з допомогою рекурентних співвідношень .....	88
Колесник В. Аналіз даних у фінансовій математиці методом кейсів.....	93
Крюков М. М., Шутівський О. М., Ляшко О. В., Андрейцев А. Ю. Застосування В-сплайнів до розв'язання задачі про деформацію тонких конічних оболонок зі скісними контурами .....	97
Кузьмін А. В., Кузьміна Н. Н. Об одном алгоритме кластерного анализа сеточного типа .....	101
Кушлик Б. Р., Кушлик-Дивульська О. І., Поліщук Н. В. Математичні аспекти методу аналітичної ієрархії.....	106
Лапач С. М. Проблеми викладання у вищій школі в умовах постнекласичної науки .....	111
Медведев К. Б., Нефьодова Г. Д., Манжелій А. Ю. Зображення параметрів кола змінної напруги на комплексній площині.....	116
Микитин М. М., Мартиняк Р. М., Середницька Х. І. Математичне моделювання взаємодії пружного півпростору і жорсткої основи за появи міжконтактного зазору по кільцевій або круговій області під дією стоків тепла ..	120
Міцюхін А. І. Кадавання інфармації на аснове выкарыстання сумежных класаў кода .....	122
Плащинська А. В. Метод наближеного розв'язку нелінійного інтегрального рівняння руху фронту руйнування внаслідок втоми в тонкій нескінченній пластині .....	125
Поліщук Н. В., Кушлик-Дивульська О. І. Аналіз надійності роботи триканальної системи масового обслуговування.....	130
Радченко С. Г., Лапач С. Н. Математическое моделирование системы кондиционирования воздуха летательного аппарата .....	134
Резник В. С. Об одном методе конкретизации функционала при определении параметров ядер наследственности в линейной теории вязкоупругости .....	138
Рожок Л. С. Напружений стан шаруватих неоднорідних порожнистих циліндрів з овальним поперечним перерізом .....	142
Селезньова Н. П., Сараєва Ю. О. Точкові оцінки числових характеристик дискретного розподілу в контексті виборів президента ..	147
Скороход Р. В., Коропов О. В. Математична модель радіаційно-індукованої сегрегації в концентрованих металевих сплавах Fe-Cr-Ni .....	153
Стоян В. А., Задорожний О. О. Про результати програмно-аналітичного моделювання динаміки неповно спостережуваних лінійних просторово розподілених систем.....	161
Фернаті П. В. Визначення параметрів ядер інтегральних операторів у нелінійній моделі в'язкопружності за їх резольвентами .....	165
Штефан Т. О., Засовенко А. В. Дослідження осаду циліндричної заготовки в умовах осесиметричної деформації .....	170
Яджак М. С. Деякі паралельні алгоритми розв'язання задач цифрової фільтрації ...	172

## Секція 2. Методика викладання математики у вищій школі

Варивода В. О., Гришко О. М., Гурнік О. О. Про деякі проблеми викладання курсу вищої математики студентам-першокурсникам технічних напрямків підготовки .....	178
Гришина В. А., Гришин В. А. Критериальный выбор методов аппроксимации в интерактивном режиме .....	183
Дем'яненко О. О., Репета Л. А. Ділові та рольові ігри як метод навчання .....	186
Дрозд В. В. Цариця навчального процесу .....	189
Дудко А. Ф., Москвичова К. К. Застосування системи GeoGebra на заняттях з вищої математики студентів технічних спеціальностей .....	192
Калайда О. Ф. Скільки існує колокант функції із простими вузлами? .....	194
Калайда О. Ф. Двосторонні дробово-раціональні колоканти із двократними вузлами .....	197
Калайда О. Ф. Лінійні двосторонні автономні методи розв'язування задачі Коші для нормальних диференціальних рівнянь .....	202
Калайда О. Ф. Двосторонні многочлени Тейлора та відповідні двосторонні квадратурні формули .....	204
Калайда О. Ф. Дробово-раціональні двосторонні методи двох дотичних розв'язування скалярних скінченних рівнянь .....	206
Калайда О. Ф. Дробово-раціональні квадратурні формули на основі дробово-раціональних колокант .....	209
Калайда О. Ф. Лінійні двосторонні методи двох дотичних розв'язування скінченних рівнянь .....	212
Калайда О. Ф. Про логарифмічні квадратурні формули .....	214
Калайда О. Ф. Матричні алгоритми чисельного диференціювання на основі дробово-раціональних колокант .....	217
Калайда О. Ф. Про одне подання многочлена типу Лагранжа за зростаючими степенями .....	220
Калайда О. Ф. Про двосторонні колоканти із простими вузлами колокації .....	222
Калайда О. Ф. Про колоканти типу Ерміта — Маркова .....	227
Калайда О. Ф. Про метод двох дотичних чисельного інтегрування функцій та задачі Коші для нормальних рівнянь .....	230
Калайда О. Ф. Про студентські науково-дослідні математичні гуртки .....	233
Калайда О. Ф. Про золотий переріз, математичне сподівання, середнє арифметичне та дисперсію .....	235
Карупу О. В., Олешко Т. А., Пахненко В. В. Про деякі особливості викладання лінійної алгебри англомовним студентам НАУ .....	237
Кучма М. І. Про один ефективний метод знаходження власних векторів матриці .....	241
Кучма М. І., Тимошенко Н. М. Псевдорозв'язність систем лінійних рівнянь і метод найменших квадратів .....	247
Лагода О. А. Прикладні задачі як стимул вивчення математики .....	252
Левізов С. В., Курбико І. Ф. Про безпосередню оцінку логарифмічних величин (порівняння деяких логарифмів) .....	256
Мохонько А. З., Васіна Л. С., Мохонько В. Д. Про систему тестових завдань для контролю знань з математики для економістів .....	260

Панасюк Н. М. <i>Чи треба вчити формули в час суцільної комп'ютеризації знань?</i> ..	265
Потемкина С. Н., Розанов А. В. <i>Модели процессов электромагнитной индукции и особенности практических расчетов на их основе</i> .....	268
Сапрікін С. М. <i>Застосування теорем Ролля, Лагранжа та Коші для розв'язання задач студентських математичних олімпіад</i> .....	273
Тригубець Б. О., Листопадова В. В. <i>Фігури Ліссажу</i> .....	276
Циганкова Г. А., Марченко С. В. <i>Аспекти викладання вищої математики для студентів технологічних спеціальностей</i> .....	279
Чепок О. О., Белітченко Д. М. <i>Концепція Нової української школи і доцільність змістової перебудови традиційної структури освітньої програми Середня освіта(Фізика) для здобувачів вищої освіти за першим (бакалаврським) рівнем</i> .....	281
Шершень Т. О., Симчук Я. В. <i>Про деякі методи обчислення інтеграла Гауса</i> .....	284

### Секція 3. Історія точних наук

Горенчук С. Т., Корзун Л. С. <i>Софія Василівна Ковалевська (1850–1891)</i> .....	289
Задерей П. В., Задерей Н. М., Нефьодова Г. Д., Калюга Б. В. <i>Академік Микола Миколайович Боголюбов (до 110-річчя від дня народження)</i> .....	292
Задерей П. В., Задерей Н. М., Нефьодова Г. Д., Ткаченко А. В. <i>Федір Петрович Ярмчук як педагог та вчений-методист (до 100-річчя з дня народження)</i> .....	297
Маловичко Т. В. <i>Мишель Рольє і метод каскадов</i> .....	301
Маловичко Т. В. <i>Семья Дж. Г. Стокса</i> .....	306
Сташенко М. О., Трачук Т. В. <i>Михайло Пилипович Кравчук як активний популяризатор науки</i> .....	311

### Секція 4. Сучасні освітні технології у вищій школі

Власенко К. В., Лов'янова І. В., Сітак І. В., Чумак О. О. <i>Про створення громадської організації «SmartMaths»</i> .....	318
Диховичний О. О., Дудко А. Ф. <i>Технологія розвитку компетентності викладачів щодо оцінювання якості тестів з вищої математики</i> .....	321
Крохмаль Т. М., Нікітенко О. М. <i>Дослідження динамічних систем з використанням системи комп'ютерної математики Maple</i> .....	325
Нестеренко О. Б. <i>До питання особистісно-орієнтованої освіти в ЗВО</i> .....	329

Наукове видання

# **МАТЕМАТИКА В СУЧАСНОМУ ТЕХНІЧНОМУ УНІВЕРСИТЕТІ**

Матеріали  
VIII Міжнародної  
науково-практичної конференції  
*26–27 грудня 2019 року*

**Технічний редактор**

Павло Кушнір  
канд. істор. наук